UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE UNITED STATES OF AMERICA, Plaintiff, -against- ROMAN STORM, ET AL., Defendant.	Case No.: 23 Cr. 430 (KPF) **Michael Perklin's Affidavit In Support of Motion to Suppress**

I, Michael Perklin, declare under penalty of perjury and pursuant to 28 United States Code, Section 1746, that the following is true and correct:

1. I have 14 years of experience with blockchain technology including cryptocurrency wallets. I have advised corporations and governments in their use. My CV is attached to this report as **Appendix A**.
2. In my experience, one of the most common misunderstandings I have observed is the (mistaken) supposition that cryptocurrency wallets "hold" cryptocurrencies in a manner similar to how physical wallets "hold" cash and cards.
3. While the term "wallet" is not always consistently applied as it pertains to cryptographically-controlled assets like cryptocurrencies, a cryptocurrency "wallet" generally refers to a software application that is designed to grant its user control over (but not custody of) some set of cryptographically-controlled assets by storing a user's cryptographic private keys[1].

[1] Custodial cryptocurrency exchanges, like Coinbase, that offer so-called "wallet services" on their platforms (like Coinbase), may operate differently than software wallets or hardware wallets. For purposes of this report, I do not include those as "wallets," and I do not believe they are at issue in the motion. Nevertheless, those "wallet services" cannot take custody of any blockchain assets either.

4. Cryptocurrency wallets provide one way to hold and manage cryptographic private keys. Private keys are very large numbers that can be up to 156 digits long[2]. These large numbers work like credentials that grant access to external systems via the Internet. While it is common to use wallet software to manage keys, it is possible (but uncommon) to store and manage private keys oneself.
5. There are different types of cryptocurrency wallets, including "software wallets" offered by companies such as MetaMask and Electrum, that rely on other hardware devices such as smartphones or computers to function. There are also "hardware wallets," such as those offered by Trezor, Ledger, or KeepKey. These hardware wallets are separate, tangible devices, similar to a USB device, that run their own software on-board a dedicated hardware device.
6. Neither software nor hardware wallets hold any cryptocurrencies, tokens, or funds of any kind. Accordingly, the word "wallet" in connection with cryptocurrency is a bit of a misnomer. Wallets only store private keys and the software needed to utilize them.
7. Units of cryptocurrency reside on their associated blockchain. Blockchains are the only structures that can have "custody" over any cryptocurrency. For example:
    A. All bitcoin in existence is held by Bitcoin's blockchain.
    B. All ether in existence is held by Ethereum's blockchain.
8. Private keys are analogous to client cards issued by modern banks (i.e. bank cards). Bank cards grant users access to external systems (the bank's systems) via merchant terminals and web applications served over the Internet.

[2] The largest private key can be calculated as (2^{512} - 1), or 13,407,807,929,942,597,099,574,024,998,205,846,127,479,365,820,592,393,377,723,561,443,721,764,030,073,546,976,801,874,298,166,903,427,690,031,858,186,486,050,853,753,882,811,946,569,946,433,649,006,084,095 which is textualized as "over 13.407 Quinquagintillion."

9. Bank cards do not themselves hold any fiat currencies or other funds of any kind. Instead, a banking client's funds are stored by their bank, and are accessible via their bank card.

10. A cryptocurrency user's cryptocurrencies are stored on that cryptocurrency's blockchain and are accessible via their private key. Like a bank card, a private key can be placed in different cryptocurrency wallets, but placing a private key in a cryptocurrency wallet does not move any cryptocurrency.

11. While it is possible to withdraw / remove funds from a bank account into a physical form (i.e. cash) and to take custody of these funds, it is not possible to remove cryptocurrencies from their respective blockchains. For this reason, "custody" of cryptocurrencies is impossible.

12. Cryptocurrency wallets can control a subset of cryptocurrencies and assign them to other keys on their blockchains. When doing so, the cryptocurrencies always remain on their respective blockchain; they are merely assigned to another key. A private key does, however, permit the user the ability to transfer, exchange, or sell the cryptocurrency by assigning it to another key in the same way a bank card permits a client to transfer dollars to another bank account.

13. When a user is said to "transfer cryptocurrency to another account," what actually occurs is a user transfers *control* over those assets from their key to another key. The assets do not move; custody of the cryptocurrency is always held by the same blockchain. The user with the key therefore has control over—but not custody of—the asset.

14. I understand that the government has stated in Docket Number 1, Paragraph 6 of the Indictment that:

> *"The Ethereum address is analogous to the account number for a bank account, while the wallet is analogous to a portfolio of bank accounts, since a single wallet can contain multiple Ethereum addresses."*

15. The above quote is not true to the extent it means to suggest that the account proceeds are *in* the wallet (like proceeds are *in* a bank account). This is similar in nature to alleging that a bank card is analogous to a portfolio of bank accounts which is equally untrue. A leather wallet on its own stores nothing, and when a bank card is placed into a leather wallet, the wallet does not suddenly have all of the money stored in that bank card's account; that money is still held by the remote bank. Similarly, a cryptocurrency wallet with a private key in it does not suddenly have all of the tokens associated with that key's account; those tokens are still held by a remote blockchain.

16. Cryptocurrency wallets do not—and cannot—store any cryptocurrencies.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge and belief.

Executed on this 29th day of March, 2024, in Toronto, Canada

Michael Perklin

Appendix A — CV of Michael Perklin

[This page intentionally left blank]

Michael Perklin, *CBP, CCSSA, CISA, CISSP, EnCE, ACE*

Contact Information

Cell: +1 (416) 992-6953
Email: mperklin@bitcoinsultants.ca
Twitter: @mperklin
LinkedIn: https://ca.linkedin.com/in/perklin

Qualifications

Michael holds the following degrees and certifications:

Master of Science in Information Assurance (MSIA), University of Davenport, Davenport, Michigan

Bachelor of Applied Information Sciences (Information Systems Security) (BaISc), Sheridan Institute, Oakville, Ontario

Computer Science Technology diploma (CST), Sheridan Institute, Oakville, Ontario

Reid Technique of Interview and Interrogation - Advanced

Certified Bitcoin Professional (CBP) #1a83e6

Certified CCSS Auditor (CCSSA) #5d3ae2

Certified Information Systems Security Professional (CISSP) #443796

Certified Information Systems Auditor (CISA) #14115468

Encase Certified Examiner (EnCE) #15-0911-4347

AccessData Certified Examiner (ACE) #UR-fc1p7132e98qw32-1229715

Affiliations

Michael is proud to be affiliated with the following organizations:

- Bitcoinsultants Inc., Principal (2012-Present)
- ShapeShift DAO, Workstream Leader (2022-Present)
- ShapeShift, Chief Information Security Officer (2017-2022)
- CryptoCurrency Certification Consortium (C4), President (2014-2021), Chairman of the Board (2021-Present)
- Rogers Communications, Lead Digital Investigator (2011-2014)
- Froese Forensic Partners / LECG (2008-2011)
- Sheridan Institute, Professor of Digital Forensics and Information Security (2012)
- Bitcoin Foundation, Director (2015-2019)
- Bitcoin Alliance of Canada, Director (2013-2016)

Relevant Experience

Michael founded Canada's first blockchain security consulting company, Bitcoinsultants, in 2012 after working in the Information-Security field for nearly a decade. Since then, he has earned an industry-wide reputation for best-in-class blockchain security consultations, and cryptocurrency security audits, and now focuses his time on Expert Witness testimony for cases related to cryptocurrencies and blockchains.

Relevant experience includes:

- Over a decade of hands-on professional experience with bitcoin, cryptocurrency and blockchain security at Bitcoinsultants Inc., the world's first blockchain security consultancy
- Served as ShapeShift's Chief Information Security Officer (CISO) from 2017-2022
- Primary author and editor of the CryptoCurrency Security Standard - a collection of security controls gleaned from the study of dozens of information systems (both breached and secured)
- Authored hundreds of reports related to digital investigations and consultations as Expert Witness
- Being deposed, cross-examined, and providing testimony as an Expert Witness in Canada, the USA, and UAE
- Lead and coordinated the world's first decentralization of an established company into a Decentralized Autonomous Organization (DAO) with ShapeShift in 2021.
- Design, implementation, and deployment of a high-security bitcoin vault system for the Ethereum crowdsale in 2014 which raised and securely stored over 30,000 BTC
- Conducted investigations into multiple high-profile breaches of cryptocurrency systems including Bitfinex and ShapeShift
- Produced the Blockchain Training Conference at multiple international locations, training lawyers, accountants, investigators and law enforcement personnel on how cryptocurrencies work (2016,2019)
- Lead a digital-forensic investigation across multiple countries that culminated in the arrest and conviction of a cryptocurrency thief in Dubai, UAE
- Software Architecture and Engineering consultation with dozens of clients designing blockchain-based information systems to ensure security and assurance of funds
- Security consultations for Initial Coin Offerings (ICOs) that launched new cryptocurrencies including Ethereum, Factom, and Zcash
- Performed source code audits of web applications to identify security vulnerabilities and misuse of cryptographic libraries
- Advised the Canadian Senate Banking Committee on bitcoin, blockchain technology and cryptocurrency investigations in 2014

Cryptocurrency and Blockchain Projects

Michael is involved in a variety of cryptocurrency related projects:

- Arkeo — A decentralized blockchain information network designed to remove central points of failure to open and public blockchain information. Michael lead the architectural design of the ShapeShift DAO's most ambitious project to replace its centralized RPC and database connections with a decentralized equivalent.
- CryptoCurrency Security Standard — The world's first formal standard for cryptocurrencies. Michael worked with industry-recognized security experts to collect and analyze information about the world's most successful and least successful cryptocurrency systems. This data was used to author the world's first standard that applies to cryptocurrencies, allowing anyone to measure a company's security practices against a common scale. Michael currently serves as the chairman of the CCSS Steering Committee.
- Certified Bitcoin Professional — The world's first personnel certification for cryptocurrencies. Michael worked with Bitcoin experts around the world to build a database of peer-reviewed exam questions for the world's first cryptocurrency certification.
- Blockchain Training Conference — The world's first blockchain conference targeted at people *outside* the blockchain industry. Michael was lead organizer of this series of training events held in countries around the world. The Blockchain Training Conference trained lawyers, accountants, developers, auditors, traders, law-enforcement personnel and anti-money-laundering specialists in how blockchains work and how work with this new technology that is sweeping the globe.
- Electrum — An open-source bitcoin wallet.
  Michael has contributed enhancements to Electrum which added a high-security feature allowing offline computers and online computers to communicate solely with QR-codes, removing the opportunity for malware to infect offline systems.

Publications

Michael has contributed the following papers to the information security community:

- "You Are What You Play": Breaching privacy and identifying users in online gaming, Transactions of the 12th Annual PST (Privacy, Security, Trust) IEEE Conference, Ryerson, Toronto, Canada, July 23-24, 2014
- Dealing with CryptoWall and Ransomware Decentral Blog, August, 2014
- Bitcoin Handbook for Non-Profits Bitcoin Foundation, October, 2014

Select Speaking Engagements

Michael has been invited to speak at more than 100 appearances worldwide. A selection of the more notable speaking engagements are listed here:

- *Everyday Opsec*
  Consensus. New York, May 2018.
- *Life in 2030*
  Blockchain Futurist. Toronto, August 2018
- *Operational Security*
  Bitcoin, Ethereum, & Blockchain Superconference, Texas, February 2018
- *Blockchain Security in 2030: A Look Forward*
  HoshoCon. Las Vegas, October 2018.
- *Blockchain Security: Past, Present, Future*
  Genesis Moscow. Moscow, September 2017
- *Thefts, Breaches, and Attacks - When Things Go Wrong*
  Blockchain:Money, London. November, 2016
- *Technology and Innovation Panel: Blockchain*
  ACAMS Canada, Toronto. Ontario, 2016
- *Blockchain Investigations*
  Blockchains, Cryptocurrencies, and AML, Toronto. August, 2016
- *The Future of Blockchains*
  Blockchain World Congress, New York. September, 2016
- *Blockchain Investigations*
  Blockchain Training Conference, Toronto. June, 2016
- *CCSS In Depth*
  Blockchain Training Conference, Toronto. June, 2016
- *Blockchains and Accounting*
  YDCPAA, Toronto. January, 2016
- *Bitcoin and Why it Matters*
  Ivey Alumni Network, Toronto. June, 2015
- *Securing Bitcoin and reaching CCSS Level III*
  Texas Bitcoin Conference, Texas. April, 2015
- *Bitcoin and Financial Technology*
  FISD Conference, New York. December, 2014
- *Bitcoin Security*
  Latin American Bitcoin Conference, Rio De Janeiro Brazil. December, 2014
- *The Bitcoin Startup Ecosystem*
  Inside Bitcoins, Las Vegas NV. October, 2014
- *Witness on Bitcoin and Cryptocurrencies Senate Committee on Banking, Trade, and Commerce*, Ottawa ON. October, 2014
- *ACL Steganography*
  Lockdown, Madison WI. June, 2014
- *High Security Bitcoin*
  Bitcoin Expo 2014, Toronto. April, 2014
- *Bitcoin - Myths and Realities.*
  Ontario Securities Commission, Toronto. February, 2014
- *The State of Cyber Security*
  FISD Conference, Toronto. November, 2013
- *Forensic Fails*
  DEF CON 21, Las Vegas. August, 2013
- *ACL Steganography*
  DEF CON 21, Las Vegas. August, 2013
- *Bitcoin 101 for Cyber Investigators*
  HTCIA Ontario Chapter, Toronto. April, 2013
- *Bitcoin for Lawyers - Up to Speed in 60m*
  [Redacted], Toronto. May, 2012
- *Anti-Forensics and Countermeasures*
  SECTOR, Toronto. October, 2012
- *Anti-Forensics and Anti-Anti-Forensics*
  DEF CON 20, Las Vegas. July, 2012
- *Defence In Depth - Don't Stop in the Middle*
  pgWest Conference, San Jose. September, 2011